Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release 25.0(4)

Introduction

If you have a private cloud, you might run part of your workload on a public cloud. However, migrating workload to the public cloud requires working with a different cloud provider interface and learning different ways to set up connectivity and define security policies. Meeting these challenges can result in increased operational cost and loss of consistency. Cisco Cloud Application Policy Infrastructure Controller (APIC) can be used to solve the these problems by extending a Cisco Multi-Site fabric to Amazon Web Services (AWS), Microsoft Azure, or Google public clouds. You can also mix AWS, Azure, and Google Cloud in your deployment.

This document describes the features, issues, and limitations for the Cisco Cloud APIC software. For the features, issues, and limitations for the Cisco APIC, see the appropriate Cisco Application Policy Infrastructure Controller Release Notes. For the features, issues, and limitations for the Cisco Multi-Site Orchestrator/Nexus Dashboard Orchestrator, see the appropriate Cisco Nexus Dashboard Orchestrator Release Notes.

For more information about this product, see " Related Content."

Note: The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Date	Description
July 9, 2022	Release 25.0(4k) became available.

New Software Features

Feature	Description
Google Cloud Statistics	Beginning with the Cisco Cloud APIC Release 25.0(4k), you can view statistics that are derived by processing Google Cloud flow logs. Available statistics include ingress and egress bytes and packets for VPCs, regions, and endpoints. For more information, see Cisco Cloud APIC for Google Cloud User Guide, Release 25.0(1) - 25.0(4).
Managed Brownfield VPC/VNETs using different access policies	This release provides updates for Managed Brownfield VPC/VNETs using the access policies in Cisco Cloud APIC with AWS and Azure, where new access policies are available at different levels. For more information, see: • Importing Existing Brownfield AWS Cloud VPCs into Cisco Cloud APIC • Importing Existing Brownfield Azure Cloud VNets into Cisco Cloud APIC
Route table copying	This release allows for route table copying when importing AWS VPCs or Azure VNets into Cisco Cloud APIC. For more information, see: • Importing Existing Brownfield AWS Cloud VPCs into Cisco Cloud APIC • Importing Existing Brownfield Azure Cloud VNets into Cisco Cloud APIC

Feature	Description
Device Connector to enable telemetry to Cisco Intersight	Support is added for telemetry from Cisco Cloud APIC to Cisco Intersight using Device Connector. For more information, see Cisco Cloud APIC and Intersight Device Connector.
Support for PAYG Licensing Model for Cisco Catalyst 8000V in Cisco Cloud APIC	Beginning with the 25.0(4k) release, Cisco Cloud APIC supports Pay-As-You-Go (PAYG) Licensing Model on Cisco Catalyst 8000V which allows users to deploy a Catalyst 8000V instance in the cloud based on the VM size and purchase the usage on an hourly basis. For this release, this feature is supported for AWS and Azure clouds. For more information, see: • Cisco Cloud APIC for AWS User Guide, Release 25.0(1) - 25.0(4) • Cisco Cloud APIC for Azure User Guide, Release 25.0(1) - 25.0(4) • Cisco Cloud APIC for AWS Installation Guide, Release 25.0(1) - 25.0(4) • Cisco Cloud APIC for Azure Installation Guide, Release 25.0(1) - 25.0(4)
Fast Convergence using Bidirectional Forwarding Detection Protocol for Cisco Hybrid Cloud deployments	This release provides a solution for faster convergence/ fast failover using Bidirectional Forwarding Detection protocol in Cisco Cloud ACI hybrid cloud deployments for AWS and Azure Cloud Direct Connect and Express Route respectively. For more information, see Improving Convergence Between On Premises ACI sites and Cloud Sites.
Configuration Drift detection	Detects and alerts when Cisco Cloud APIC-managed configurations have been modified in cloud outside of Cisco Cloud APIC. For more information, see: • Cisco Cloud APIC for AWS User Guide, Release 25.0(1) - 25.0(4) • Cisco Cloud APIC for Azure User Guide, Release 25.0(1) - 25.0(4)

Supported Upgrade Paths

Cisco Cloud APIC supports policy-based upgrades for the following upgrade paths for AWS and Azure:

- Release 5.2(1) to 25.0(4)
- Release 25.0(1) to 25.0(4)
- Release 25.0(2) to 25.0(4)
- Release 25.0(3) to 24.0(4)

Changes in Behavior

There are no changes in behavior in this release.

Open Issues

Click the bug ID to access the Bug Search tool and see additional information about the bug. The " Exists In" column of the table specifies the 25.0(4) releases in which the bug exists. A bug might also exist in releases other than the 25.0(4) releases.

Bug ID	Description	Exists in
CSCvo30542	TACACS monitoring of the destination group is not supported through the GUI.	25.0(1c) and later
CSCvu64277	Stats seen on Cisco Cloud APIC are sometimes not in sync with Azure stats.	25.0(1c) and later
CSCvu66521	In the " Cloud Resources" section of the GUI, the names displayed in the " Name" column are not the same as the name of resources on the cloud. These are showing the Cloud APIC object names.	25.0(1c) and later
CSCvu72354	Adding an EPG endpoint selector fails with an error message saying the selector is already attached.	25.0(1c) and later
CSCvu78074	Route nextHop is not set to the redirect service node specified in the service graph.	25.0(1c) and later
CSCvv32664	When the CSR bandwidth needs to be increased, the user needs to undeploy all the CSRs in all the regions and redeploy with the desired bandwidth, which can cause traffic loss.	25.0(1c) and later
CSCvx16601	When the " AllowAll" flag is enabled on a service device such as a native load balancer or on the logical interface of a third party device, it is possible that to see some specific rules apart form a rule that allows all traffic from any source to any destination.	25.0(1c) and later
CSCvy06610	The eventmgr crashes when handling a fault triggered by a new cloud account.	25.0(1c) and later
CSCvy45517	The Cisco Cloud APIC GUI shows the total allowed count for CtxProfile, VRF (fvCtx), EPGs, and contracts. These numbers have been validated only for Azure-based deployments. For AWS deployments, the numbers supported are much lower.	25.0(1c) and later
CSCvy89617	Cloud routers may not get created if external network objects are not configured. External network configuration is required for configuring cloud routers.	25.0(1c) and later

Bug ID	Description	Exists in
CSCvy97972	Cisco Cloud APIC in this release limits the number of regions where we can deploy the hubnetwork in order to establish external connectivity. When you attempt to deploy/configure hubnetwork in more than four regions, the configuration will be rejected with the following error: Invalid Configuration CT_INTNETWORK_REGION_MAXIMUM: At present, there can be at most 4 cloudRegionName in cloudtemplateIntNetwork uni/tn-infra/infranetwork-default/intnetwork-default; current count = <total-hubnetwork-regions-attempted>	25.0(1c) and later
CSCvz17160	Customers are restricted to shorter key value pairs than they need to be.	25.0(1c) and later
CSCvz21771	VPN tunnels may not come up when the Cisco Cloud APIC configuration is posted via XML interface. This problem won't be seen/encountered when we use the Cisco Cloud APIC UI.	25.0(1c) and later
CSCvz38067	Incorrect DNS server is configured on Cisco Cloud APIC with Google Cloud. Though this is not directly used when deploying Cisco Cloud APIC with Google Cloud, an incorrect IP address is configured.	25.0(1c) and later
CSCvz47166	When delete followed by add operations of tenant or other resources (such as VPCs and contracts) are done within a short span of time, it is possible that the resource deployment in Google Cloud may get out of sync with the configuration on Cisco Cloud APIC. The likelihood of this happening is directly proportionate to the scale of configuration and how quickly the operations are done. We may see resources either not created or not deleted on Google Cloud to match the user configuration on Cisco Cloud APIC.	25.0(1c) and later
CSCvz52773	When performing a Cisco Cloud APIC upgrade (but not also performing a CSR upgrade), before the upgrade is finished and when the Cisco Cloud APIC is reconciling the CSR configurations, if you delete certain configurations and add the same configurations back (for example, if you delete a VRF and add the VRF back), a traffic drop may happen. Eventually it should recover.	25.0(1c) and later
CSCvz62225	When you scale up the number of CSRs or routers per region, some of the configurations may be missing on the newly created CSR. This issue happens randomly on the newly created CSRs, in this case tunnels or BGP sessions on the new CSRs may be down due to missing configuration.	25.0(1c) and later
CSCwa03277	When the brownfield VPC is imported into Cisco Cloud APIC, you need to take care of the creation and management of the route table and route table entries, security group rules, and transit gateway VPC attachment. After creating the transit gateway VPC attachment with the infra transit gateway for the brownfield VPC in the AWS console, the corresponding cloudCtxPeerOper for the brownfield cloud context profile will move from Failed state to Configured state. After that, if the created transit gateway attachment for the brownfield VPC is deleted in the AWS console, cloudCtxPeerOper is not moving back to Failed state.	25.0(2e) and later

Bug ID	Description	Exists in
CSCwa07078	When the brownfield VPC is imported into Cisco Cloud APIC via REST API POST, a new cloud context profile is created. Under this cloud context profile, cloudRsCtxToAccessPolicy is created, which is in relation to read only access policy. One or more cloudCIDRs and cloudBrownfield with cloudIDMapping, which holds the VPC ID, is posted to Cloud APIC. cloudIDMapping, which contains the VPC ID, points to the VPC present in the cloud. If the VPC ID is non-existent or if there is any difference between the cloudCIDRs posted vs the CIDRs present in the VPC, cloudCtxOper and cloudCidrOper moves to a Failed state. But because of the delegate's distinguished name, the imported unmanaged VPC shows healthy.	25.0(2e) and later
CSCwa08564	UI dashboard shows the wrong status for inter-region connectivity.	25.0(2e) and later
CSCwa10752	When CSRs are deployed in non-home regions, and no CSR is deployed in the home region (where Cloud APIC is deployed) in Azure, faults are seen in the Cloud APIC where the ssh connectivity to the CSR is down.	25.0(2e) and later
CSCwa26716	An external endpoint group of type non internet cannot leak all routes(or public internet IPs) to a cloud endpoint group. This results in creating a static route in the Vnet route table to point to CSR NLB for that destination CIDR. If it's leak-all, we configure 0.0.0.0/0 to point to CSR NLB. In case of Azure Cloud APIC we do not create a static route to internet, Azure does this implicitly by default. Cloud APIC only programs the rules. When a user creates a contract or route leak, Cloud APIC programs a static route to CSR NLB. This overrides the Azure implicit default route to internet if the CIDR overlaps with the pubic internet IPs, since the leak-all creates a 0.0.0.0/0 route to point to CSR NLB. This is an invalid configuration unless the user intended it, i,e the user intended to login to the VM through it's private IP through CSR. If not the user has to leak specific routes to the cloud endpoint group.	25.0(2e) and later
CSCwa28888	This issue is hit in some cases where Cloud APIC is unable to deploy infra configuration, such as creating cloud routers in overlay-1 VPC. This is sometimes seen in new deployments, but not in the case of upgrade scenario. Cloud routers and other configurations do not get deployed in Google Cloud.	25.0(2e) and later
CSCwa29007	In the TGW l3out configuration, modifying the IPsec tunnel pre-shared key is not supported. UI does not allow the modification of the IPsec tunnel pre-shared key, as this field is grayed out. API accepts this modification of the IPsec tunnel pre-shared key, but it's not updated on the AWS.	25.0(2e) and later
CSCwa36940	Transit gateway external connectivity is not getting deployed in regions where cloud context profiles are deployed.	25.0(2e) and later
CSCwa40705	When an IKEv1 tunnel is configured to a destination while another tunnel already exists to the same destination but with a different source interface, this tunnel will remain with the protocol shown as down.	25.0(2e) and later
CSCwa40843	Stale IPsec configuration remains when an IKEv1 IPsec tunnel is deleted.	25.0(2e) and later

Bug ID	Description	Exists in
CSCwa43845	This issue occurs if there is a misconfiguration done where the local subnet was provided under routes leaked from external VRF to internal VRF. This is an Azure Cloud APIC only issue, since AWS does not allow programming routes that overlap with VPC's CIDR.	25.0(2e) and later
CSCwa44822	When the tunnels are created from source interface Gig 2 or 4, we put allow all for security group. In future the allow all rule needs to be removed and provide explicit IP needs to be allowed.	25.0(2e) and later
CSCwa45047	This is not a functional issue. There will be no fault shown in the Cloud APIC UI if the border gateway protocol sessions of the transit gateway external connectivity are down.	25.0(2e) and later
CSCwa48929	If Cloud APIC is rebooted, in a rare case an expected rule may not be programmed on the cloud due to a timing mismatch in the reconcile and programming workflow.	25.0(2e) and later
CSCwa49263	In VPC route table, the route table entry for a destination CIDR pointing to transit gateway is sometimes missing when a quick delete and add of tenant or contract is done or when we move from transit gateway connect to legacy transit gateway solution. This happens only with legacy transit gateway solution in either of the cases. This is a timing issue with the legacy transit gateway solution, where we create two transit gateways per hub network in a region. This can happen either if we move to legacy transit gateway solution or if legacy transit gateways are coming up for the first time. These conditions result in deleting the route table entry for a given destination CIDR and adding back the same entry at the same time. Due to an issue with the AWS API which returns a deleted route table entry as a non deleted entry, Cloud APIC deletes the wrong entry.	25.0(2e) and later
CSCwa97027	Sometimes the Cloud APIC CSR/CCR " Instance Status" in " Cloud Resources ->Instances -> is shown as " Not-applicable" .	25.0(3k) and later
CSCwa99935	Disabling " Hub peering" triggers a CSR deployment, which restricts the CSR count and increases the bandwidth together in a single action.	25.0(3k) and later
CSCwa18353	The route between the internal and external VRF is not programmed on the CSR. It is expected to be configured on CSR as a part of the leakTo subnet configuration.	25.0(4k) and later
CSCwa92033	Cisco Catalyst 8000V License is not getting deregistered from Cisco Smart License Server as the Cisco Catalyst 8000V lose connection to the internet before getting deleted.	25.0(4k) and later
CSCwa97199	No functional issue, stale licenses are configured on the Cisco Catalyst 8000V. On programming a T2 license on the Cisco Catalyst 8000V, a stale license entry is seen on both the Cisco Catalyst 8000V and the Cisco Smart account.	25.0(4k) and later
CSCwa99599	On Azure, it takes a long time for Cisco Catalyst 8000Vs to become ready when deployed in a new region. As a result, the inter-site tunnels take time to come up, delaying the traffic.	25.0(4k) and later
CSCwb01378	The following fault appears on the Cisco Cloud APIC indicating that the license is not configured on the CCR : Oper State of HcplatformLicense is down with administrative-down.	25.0(4k) and later

Bug ID	Description	Exists in
CSCwc01909	When staying on the VRFs table, the VRF internal/external statuses sometimes do not update for a long time.	25.0(4k) and later
CSCwc11244	In this case the HcloudCtxOper of infra VNet, which is used to deploy NLB/ALB, is down. Since one of the network interface associated with the Vnet is in a failed state, Cisco Cloud APIC is unable to add a new Cidr to the VNet.	25.0(4k) and later
CSCwc15976	When we have a contract whose resource name does not match regex '(?:[a-z](?:[-a-z0-9]{0,61}[a-z0-9])?)', it raises a fault with the following message, "Must be a match of regex '(?:[a-z](?:[-a-z0-9]{0,61}[a-z0-9])?)', invalid" , as received from the specific cloud. The details on the exact mismatch are missing from the fault.	25.0(4k) and later
CSCwc28787	When BFD is enabled between sites, the BFD sessions go down and come back up quickly with no user intervention/trigger.	25.0(4k) and later
CSCwc30301	Cloning of route-table entries to Cloud APIC route-table does not port route-table associations with other entities, such as managed-prefix-lists in AWS, SecurityGroup in Azure, and other such entities. This issue appears when the user imports a VPC/VNet into Cloud APIC in Routing Only mode or Routing & Security mode and clones the route-table(s) into an already-imported VPC/VNet.	25.0(4k) and later
CSCwc39392	In a few specific cases, on importing a brownfield VNet with a Routing & Security access policy, an NSG might not get created and/or VNets might not peer.	25.0(4k) and later
CSCwc43147	Azure vWAN feature is available on the Cloud APIC Setup Region Management screen.	25.0(4k) and later

Resolved Issues

Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Fixed In" column of the table specifies whether the bug was resolved in the base release or a patch release.

Bug ID	Description	Fixed in
CSCvz87367	Even though the preferred DNS server is taking into effect in Cloud APIC, the DNS server which was configured first continues to be the preferred DNS server.	25.0(4k)
CSCwa54001	When a quick delete and add of inter-site connectivity happens in such a way that the tunnels on the cloud are unchanged, the status on the UI may show tunnels as down even when the tunnels are up on the GCP cloud and the Azure CSR. This issue might also happen during an upgrade and/or connector restart or a crash.	25.0(4k)

Known Issues

Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Exists In" column of the table specifies the 25.0(4) releases in which the bug exists. A bug might also exist in releases other than the 25.0(4) releases.

Bug ID	Description	Exists in
CSCvo06626	When a cloudExtEpg matches on a 0/0 network and has a bi-directional contract with two cloud EPGs, such as cloudEpg1 and CloudEpg2, this can result in inadvertent communication between endpoints in cloudEpg1 and cloudEpg2 without a contract between the two EPGs themselves.	25.0(1c) and later
CSCvo55112	Logs are lost upon stopping the Cloud APIC instance.	25.0(1c) and later
CSCvo95998	There is traffic loss after a Cloud APIC upgrade. Traffic will eventually converge, but this could take a few minutes.	25.0(1c) and later
CSCvq11780	Creating VPN connections fail with the "invalidCidr" error in AWS or the "More than one connection having the same BGP setting is not allowed" error in Azure.	25.0(1c) and later
CSCvq76039	When a fault is raised in the Cloud APIC, the fault message will be truncated and will not include the entire cloud message description.	25.0(1c) and later
CSCvr01341	REST API access to the Cloud APIC becomes delayed after deleting a tenant with scaled EPGs and endpoints. The client needs to retry after receiving the error.	25.0(1c) and later
CSCvu05329	The Ctx Oper managed object is not deleted after the attachment is deleted.	25.0(1c) and later
CSCvu81355	Traffic gets dropped after downgrading to the 5.0(1) release. Cloud Services Router has incompatible configurations due to an issue with reading configurations using SSH.	25.0(1c) and later
CSCvu88006	On the Dashboard, fewer VNet peerings are shown than expected.	25.0(1c) and later
CSCvv81647	When an invalid Cloud Services Router license token is configured after initially configuring a valid token, the Cloud Services Router fails the license registration and keeps using the old valid token. This failure can only be found from the CSR event log.	25.0(1c) and later
CSCvw05821	Redirection and UDR does not take effect when traffic coming through an express route and destined to a service end point is redirected to a native load balancer or firewall.	25.0(1c) and later
CSCvw07392	Inter-site VxLAN traffic drops for a given VRF table when it is deleted and re-added. Packet capture on the CSR shows "Incomplete Adjacency" as follows: Punt 1 Count Code Cause 1 10 Incomplete adjacency <<<<<<< Drop 1 Count Code Cause 1 94 Ipv4NoAdj	25.0(1c) and later
CSCvw07781	There is complete traffic loss for 180 seconds.	25.0(1c) and later
CSCvw24376	Inter region traffic is black-holed after the delete trigger for contracts/filter. It was observed that the TGW entry pointing to the remote region TGW is missing for the destination routes. On further debugging it was found that post delete trigger as part of re-add flow, when a describe call is sent to AWS got a reply with the state of this entry as "active" because of which a new create request is not being sent.	25.0(1c) and later
CSCvw39814	Infra VPC subnet route table entry for 0.0.0.0/0 route with TGW attachment as nh, is left as a stale entry upon being undeployed. There is no functional impact. Upon being redeployed, this entry is updated with the correct TGW attachment ID as nh.	25.0(1c) and later

Bug ID	Description	Exists in
CSCvw40737	SSH to a virtual machine's public IP address fails, despite the NSG allowing the traffic inbound. SSH to the private IP address of the virtual machine from within the VNet works.	25.0(1c) and later
CSCvw40818	After upgrading Cloud APIC, the Cloud Services Routers will be upgraded in two batches. The even set of CSRs are triggered for upgrade first. AFTER their upgrade is complete and all of the even CSRs are datapathReady, only then the odd set of CSRs will be triggered for upgrade. When even one of the upgrade of the even CSRs fail and they don't become datapathReady, the odd set of CSRs will not be triggered for upgrade. This is the behavior followed to avoid any traffic loss.	25.0(1c) and later
CSCvw48190	When Cloud APIC is restart, the VPN connection from a tenant's VNets will get deleted and re-created, one by one. This can be seen in the Azure activity logs. It should not impact traffic, as all connections are not deleted at the same time.	25.0(1c) and later
CSCvw49898	When the downgrading from the 5.2(1) release to the 5.0(2) release, traffic loss is expected until all of the CSRs are downgraded back to the 17.1 release. The traffic loss occurs because when the CSRs are getting downgraded to the 17.1 release, the CSR NIC1s will be in the backendPools and traffic from the spokes will still be forwarded to the native load balancer. The traffic gets blackholed until the CSRs get fully programmed with all the configurations in the 17.1 release.	25.0(1c) and later
CSCvw50918	Upon downgrading Cloud APIC, VPN connections between Cloud APIC and the cloud (AWS/Azure VPN gateway) will be deleted and re-created, causing traffic loss. Traffic loss is based on how quickly the VPN connections are deleted and re-created in AWS due to AWS throttling.	25.0(1c) and later
CSCvw51544	A user who is assigned a large number of security domains may not be able to create other Cisco ACI policies.	25.0(1c) and later
CSCvw55088	A user who is assigned a large number of security domains may not be able to create other Cisco ACI policies.	25.0(1c) and later
CSCvx91010	When TGW Connect is disabled, traffic loss is observed for about 8 minutes.	25.0(1c) and later
CSCvx98260	When delete followed by add operations of tenant or other resources (such as VPCs and contracts) are done within a short span of time, it is possible that the resource deployment in Google Cloud may get out of sync with the configuration on Cisco Cloud APIC. The likelihood of this happening is directly proportionate to the scale of configuration and how quickly the operations are done. We may see resources either not created or not deleted on Google Cloud to match the user configuration on Cisco Cloud APIC.	25.0(1c) and later
CSCvy10936	Downgrading Cisco Cloud APIC from release 5.2(1) to 5.1(2) may cause CSRs to not be downgraded. The CSR release for 5.2(1) is 17.3.2, and the CSR version for release 5.1(2) is 17.3.1. After the Cisco Cloud APIC downgrade, the CSR version should be downgraded to 17.3.1, but it will not happen due to this bug.	25.0(1c) and later
CSCvy12722	Loss of traffic between a cloud and Cisco ACI On-Premises deployment.	25.0(1c) and later
CSCvy13369	After upgrading AWS, infra vPC peering does not get deleted.	25.0(1c) and later
CSCvy19286	There is traffic loss after downgrading from 5.2(1) to 5.1(2).	25.0(1c) and later

Bug ID	Description	Exists in
CSCvy28890	There is a loss in SSH connectivity to the Cisco Cloud APIC across reboots. But, after a few minutes, the connection should come back and users will be able to SSH in to the Cisco Cloud APIC again.	25.0(1c) and later
CSCvy28896	There is an increase in the connector's memory utilization. All of the CSR workflows rerunning might happen even after the setup is in the steady state.	25.0(1c) and later
CSCvy30314	After upgrading the Cisco Cloud APIC, on the TGW route tables, the default route (0.0.0.0/0) does not point to infra VPC attachment or is missing. In this case, traffic intended to get forwarded to the CSR will be dropped or forwarded to an invalid next-hop.	25.0(1c) and later
CSCvy33435	There is intersite traffic loss when TGW Connect is enabled.	25.0(1c) and later
CSCvy34180	Cloud Intersite traffic is dropped due to the CSR in the cloud site not advertising the EVPN routes.	25.0(1c) and later
CSCvy77233	Routes for subnets that are not yet configured in Google Cloud may become visible on an external device. When you configure routes to be advertised to an external device, but don't actually configure subnets in the cloud that you intend to advertise the routes for, those routes are still advertised. Remote router may see routes that are advertised even when the subnets are not yet configured. The traffic will get dropped because the subnets are not actually configured.	25.0(1c) and later
CSCvz11574	The cloud VRF egress route table is missing the route for 0.0.0.0/0 via the Internet Gateway (IGW), which leads to issues with ssh for VMs in the cloud VRF.	25.0(1c) and later
CSCvz20282	An upgrade to or downgrade from the Cloud APIC 5.2(1g) release to any release while using " Ignore Compatibility Check: no" will fail. The following fault is raised: " The upgrade has an upgrade status of Failed Due to Incompatible Desired Version."	25.0(1c) and later
CSCvz49747	When delete followed by add operations of tenant or other resources (such as VPCs and contracts) are done within a short span of time, it is possible that the resource deployment in Google Cloud may get out of sync with the configuration on Cisco Cloud APIC. The likelihood of this happening is directly proportionate to the scale of configuration and how quickly the operations are done. We may see resources either not created or not deleted on Google Cloud to match the user configuration on Cisco Cloud APIC.	25.0(1c) and later
CSCwa92698	If the Cloud APIC infra CIDR has a collision with the reserved CIDR 172.17.0.0/16, connectivity to the Cat8kv VMs from Cloud APIC VM might fail. If the connectivity fails, the configuration push to Cat8kv will fail and Cat8kv will remain unreachable from Cloud APIC. A fault will be raised in the Cloud APIC. Currently 172.17.0.0/16 is reserved by Cloud APIC and it cannot be used as Infra CIDR. 172.17.0.0/16 is used by the docker network running on Cloud APIC.	25.0(3k) and later

Compatibility Information

This section lists the compatibility information for the Cisco Cloud APIC software. In addition to the information in this section, see the appropriate Cisco Application Policy Infrastructure Controller Release Notes and Cisco Nexus Dashboard Orchestrator Release Notes for compatibility information for those products.

- Cloud APIC release 25.0(4k) is compatible with Cisco Nexus Dashboard Orchestrator, release 3.7(1).

- Cloud APIC supports the following AWS regions:
    - Asia Pacific (Hong Kong)
    - Asia Pacific (Mumbai)
    - Asia Pacific (Osaka-Local)
    - Asia Pacific (Seoul)
    - Asia Pacific (Singapore)
    - Asia Pacific (Sydney)
    - Asia Pacific (Tokyo)
    - AWS GovCloud (US-Gov-West)
    - Canada (Central)
    - EU (Frankfurt)
    - EU (Ireland)
    - EU (London)
    - EU (Milan)
    - EU (Stockholm)
    - South America (São Paulo)
    - US East (N. Virginia)
    - US East (Ohio)
    - US West (N. California)
    - US West (Oregon)
- Cloud APIC supports the following Azure regions:
    - Australiacentral
    - Australiacentral2
    - Australiaeast
    - Australiasoutheast
    - Brazilsouth
    - Canadacentral
    - Canadaeast
    - Centralindia
    - Centralus
    - Eastasia
    - Eastus

- Eastus2
- Francecentral
- Germanywestcentral
- Japaneast
- Japanwest
- Koreacentral
- Koreasouth
- Northcentralus
- Northeurope
- Norwayeast
- Southafricanorth
- Southcentralus
- Southeastasia
- Southindia
- Switzerlandnorth
- Uaenorth
- Uksouth
- Ukwest
- Westcentralus
- Westeurope
- Westindia
- Westus
- Westus2

- Cloud APIC supports the following Azure Government cloud regions:
  - US DoD Central
  - US DoD East
  - US Gov Arizona
  - US Gov Texas
  - US Gov Virginia

Note: The US Gov Iowa region is not supported in Cisco Cloud APIC because Azure has deprecated support for this region.

- Cloud APIC supports all Google Cloud regions.

Related Content

See the Cisco Cloud Application Policy Infrastructure Controller page for the documentation.

See the Cisco Application Policy Infrastructure Controller (APIC) page for the verified scability, Cisco Application Policy Infrastructure Controller (APIC), and Cisco Multi-Site Orchestrator (MSO) documentation.

The documentation includes installation, upgrade, configuration, programming, and troubleshooting guides, technical references, release notes, and knowledge base (KB) articles, as well as other documentation. KB articles provide information about a specific use case or a specific topic.

By using the " Choose a topic" and " Choose a document type" fields of the APIC documentation website, you can narrow down the displayed documentation list to make it easier to find the desired document.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to apic-docfeedback@cisco.com. We appreciate your feedback.

Legal Information